Umsetzungsfahrplan der DSGVO

Datenschutz mit modernster Cybersicherheit

TREND MICRO-HAFTUNGSAUSSCHLUSS

Die Informationen in diesem Dokument sind nur zu allgemeinen und Bildungszwecken vorgesehen. Sie sind nicht als juristischer Ratgeber gedacht und sollten auch nicht als solcher angesehen werden. Die Informationen in diesem Dokument gelten möglicherweise nicht für alle Situationen und stellen unter Umständen nicht die aktuellste Situation dar. Keine enthaltenen Informationen sollten ohne vorherigen Rechtsbeistand zu den jeweiligen Fakten und Umständen als Basis oder Grundlage für Handlungen genutzt werden, und nichts davon sollte dahingehend ausgelegt werden. Trend Micro behält sich das Recht vor, die Inhalte dieses Dokuments jederzeit und ohne vorherigen Hinweis zu ändern.

Übersetzungen von Materialien in andere Sprachen werden ausschließlich als Hilfsmittel angeboten. Die Genauigkeit von Übersetzungen wird weder garantiert noch impliziert. Falls Sie Fragen zur Genauigkeit einer Übersetzung haben, sehen Sie sich bitte die offizielle Version des Dokuments in der Originalsprache an. Abweichungen oder Unterschiede in der übersetzten Version sind nicht bindend und haben keine rechtlichen Auswirkungen auf Compliance- oder Durchsetzungszwecke.

Trend Micro unternimmt zwar angemessene Anstrengungen, in diesem Dokument genaue und aktuelle Informationen anzugeben. Allerdings übernimmt Trend Micro keinerlei Haftung oder Ansprüche jeglicher Art in Bezug auf die Genauigkeit, Aktualität oder Vollständigkeit. Sie stimmen zu, dass der Abruf und Ihre Nutzung dieses Dokuments sowie die Verwendung der enthaltenen Inhalte auf eigenes Risiko erfolgt. Trend Micro übernimmt keinerlei Garantie, ob ausdrücklich oder stillschweigend. Weder Trend Micro noch irgendwelche Dritten, die bei der Erstellung, Produktion oder Bereitstellung dieses Dokuments mitgewirkt haben, haften für Folgen, Verluste oder Schäden, einschließlich direkter, indirekter, besonderer oder nachfolgender, entgangenen Gewinn oder besondere Schäden, die sich aus dem Abruf, der Nutzung, der Nichtnutzung oder im Zusammenhang mit der Nutzung dieses Dokuments, irgendwelcher Fehler oder Auslassungen in den Inhalten ergeben. Durch Nutzung dieser Informationen wird die Nutzung „wie besehen“ akzeptiert.

Inhalt

4
Zusammenfassung

5
Was ist die Datenschutz-Grundverordnung (DSGVO)?

6
Folgen der DSGVO verstehen

10
Stellt die DSGVO neue Risiken heraus?

12
Der Ablauf zur Einhaltung

14
Datenschutz als Konzept

16
Cybersicherheit im Kontext der DSGVO

19
Bereit für die DSGVO dank intelligenter, optimierter und vernetzter Abwehr

20
So kann Trend Micro helfen

22
Das Puzzle zusammensetzen: Jetzt geht es los

Zusammenfassung

Da weniger als ein Jahr bis zum Beginn der Durchsetzung verbleibt, stellt sich die EU-Datenschutz-Grundverordnung (DSGVO) schon jetzt als langwierige Aufgabe für globale Unternehmen heraus, denn sie zwingt sie, personenbezogene Daten aller Bürger des Europäischen Wirtschaftsraums, mit denen sie Geschäftsbeziehungen haben, zu schützen. Wegen unspezifischen Angaben darüber, wie "alle Daten geschützt" werden – die DSGVO ist kein Technologiestandard und fördert keine speziellen technologischen Ansätze – herrscht viel Unsicherheit nicht nur in Bezug auf den besten Ansatz, sondern auch auf die ersten Schritte.

Damit Unternehmen zu einem besseren Verständnis der Rolle von Cybersicherheit im Kontext der DSGVO gelangen können, bietet dieses Whitepaper eine allgemeine Übersicht der Verordnung sowie ein Rahmenwerk, durch das Sie bei Ihren ersten Schritten in Richtung Compliance unterstützt werden. Als Teil dessen geht es in diesem Dokument vorrangig um Tipps, wie sich moderne Cybersicherheit nutzen lässt und was sie für Unternehmen bedeutet, die das Puzzle zusammensetzen, um schlussendlich mit der DSGVO konform zu sein. Als Unterstützung für IT- und Compliance-Experten, die ein kritischer Teil des „DSGVO-Teams“ in jedem Unternehmen sind, werden die zusätzlichen Vorteile einer angemessenen Cybersicherheitsstrategie besprochen. Außerdem wird die tragende Rolle verdeutlicht, die Trend Micro in Sachen Compliance – und darüber hinaus – spielen kann.

Wichtige Erkenntnisse

- **Neue Pflichten, neue Rechte.** In aller Welt müssen Unternehmen, die personenbezogene Daten von EU-Bürgern erfassen oder verarbeiten, die Bestimmungen der DSGVO einhalten. Dies führt zu neuen Pflichten für Unternehmen sowie zu dem Erfordernis, die neuen Rechte zu unterstützen, die betroffenen Personen gewährt werden.

- **Datenschutz als Konzept.** Datenschutz muss direkt in die Implementierung jeder Aktion und jedes Projekts integriert sein, bei denen es um personenbezogene Daten geht. Daher muss der Datenschutz während der Konzeptphase von Informationstechnologien, -prozessen und -systemen eine hohe Priorität haben.

- **Abschreckende Strafen.** Werden die Bestimmungen nicht eingehalten, kann dies zu beträchtlichen Strafen, Reputationsverlust, Einstellung der Datenverarbeitung sowie Einreichung von Beschwerden durch Einzelpersonen zur Folge haben.

- **Mehrere Beteiligte.** Auf dem Weg zur Compliance sollte es um drei Hauptbereiche gehen – Recht und Compliance, Daten sowie Technologie. Dazu kommen idealerweise Beteiligte aus dem gesamten Unternehmen miteinander ins Gespräch.

- **Keine Wunderwaffe.** Jeder Aktionsplan erfordert eine Vielzahl von Aufgaben, z. B. die Zuordnung von Daten, die Bewertung der Bereitschaft, Probleme mit der Zuständigkeit und Verantwortung, die Überprüfung von Vorgehensweisen für Datenmanagement und vieles mehr.

- **Modernste Cybersicherheit.** Cybersicherheit sollte intelligent, optimiert und vernetzt sein. Sie muss sich auf mehrere Ebenen erstrecken und eine weiträumige Integration, aussagekräftige Sicherheitsanalysen, gemeinsame Nutzung von Daten über Bedrohungen, Zusammenarbeit zwischen Sicherheitslösungen, Funktionen zur Reaktion auf Vorfälle in Echtzeit sowie zentralisierte Transparenz ermöglichen. Doch was am wichtigsten ist: Die Definition, was „modern“ ist, ändert sich im Laufe der Zeit – ein Konzept, das unerlässlich für die Erstellung einer effektiven Sicherheitsstrategie für die DSGVO ist.

Was ist die DSGVO?

In den vergangenen Jahrzehnten hat sich das Problem des Datenschutzes in ganz Europa als wahre Herausforderung erwiesen. Im Bundesland Hessen trat 1970 das weltweit erste Datenschutzgesetz in Kraft, und viele anderen Bundesländer und dann auch andere Länder in Europa folgten. Im Jahr 1995 trat in der Europäischen Gemeinschaft – dem Vorgänger der Europäischen Union – derzeitige EU-Datenschutzrichtlinie in Kraft. Sie sollte nationale Gesetze angleichen und Handelsbarrieren in Europa abbauen. Allerdings setzten die Mitgliedsstaaten der Europäischen Gemeinschaft die Richtlinie mit nuancierten Unterschieden um. Dies führte zu unabhängigen nationalen Gesetzen und förderte die Inkonsistenz zwischen den Staaten. Nach vier Jahren Arbeit zielt die **EU-Datenschutz-Grundverordnung** (DSVGO), die im April 2016 eingesetzt wurde, darauf ab, die datenschutzrechtliche Gesetzgebung in der gesamten Europäischen Union (EU) zu vereinheitlichen[1] und Datenschutzgesetze so zu ändern, dass zuvor nicht vorhergesehene Datennutzungspraktiken abgedeckt werden. Die DSGVO tritt am 25. Mai 2018 in Kraft. Dieses kommende Datum mit hoher Bedeutung verlangt, dass Unternehmen – sowohl Großunternehmen als auch kleine und mittelständische Unternehmen (KMU) und sogar Einzelunternehmer ihre Datenverarbeitungskontrollen neu bewerten und einen Plan aufstellen, Compliance zu erzielen.

> „Damit in der Union ein gleichmäßiges Datenschutzniveau für natürliche Personen gewährleistet ist und Unterschiede, die den freien Verkehr personenbezogener Daten im Binnenmarkt behindern könnten, beseitigt werden, ist eine Verordnung erforderlich, die für die Wirtschaftsteilnehmer […] Rechtssicherheit und Transparenz schafft [und] natürliche Personen in allen Mitgliedsstaaten mit demselben Niveau an durchsetzbaren Rechten [und Pflichten] ausstattet."

Quelle: Zusammenfassung der Präambel 13 der Datenschutz-Grundverordnung, 27. April 2016

1. Tatsächlich gilt die DSGVO für den Europäischen Wirtschaftsraum (Staaten der Europäischen Union sowie Island, Liechtenstein und Norwegen).

Folgen der DSGVO verstehen

Die DSGVO mit ihrer Sammlung neuer Regeln und Vorschriften wirkt sich auf alle Unternehmen aus, die personenbezogene Daten verarbeiten. Die Rechtsprechung gilt für alle Unternehmen, innerhalb und außerhalb der EU, die mit personenbezogenen Daten von betroffenen Personen aus der Union zu tun haben. Sowohl Verantwortliche – die die Gründe und Mittel zur Verarbeitung personenbezogener Daten bereitstellen – als auch Auftragsverarbeiter – die die Informationen im Auftrag des Verantwortlichen speichern, digitalisieren und verarbeiten – sind verantwortlich für die Verwaltung der riesigen Mengen personenbezogener Daten, für die eine Einhaltung der DSGVO erforderlich ist. Die Verordnung wird konsistent in jedem Mitgliedsstaat angewendet, was zu beträchtlichen neuen geschäftlichen Verpflichtungen führt, die für Unternehmen und Bürger spürbar sind.

Verpflichtungen für Unternehmen

Erweiterter Gültigkeitsbereich	Die DSGVO gilt für alle Unternehmen, die mit personenbezogenen Daten von betroffenen Personen aus der EU zu tun haben, und verfeinert die Definition dessen, was „personenbezogene Daten“ ausmacht. Dies schließt Unternehmen innerhalb UND außerhalb der EU ein.
Benachrichtigung bei Datenschutz-verletzungen	Verletzungen des Schutzes personenbezogener Daten müssen der DSGVO-Aufsichts-behörde binnen 72 Stunden gemeldet werden. Betroffene Einzelpersonen müssen ebenfalls benachrichtigt werden, falls ihre Rechte und Freiheiten verletzt wurden.
Datenschutz-Folgen-abschätzungen	Datenschutz-Folgenabschätzungen sind erforderlich, um Datenschutzrisiken für Einzelpersonen zu identifizieren, wenn ihre personenbezogenen Daten erfasst, genutzt, verarbeitet und offengelegt werden.
Datenschutz-beauftragter	Unternehmen müssen einen Datenschutzbeauftragten benennen, der bei der internen oder ausgelagerten Datenverarbeitung zuständig für die Verwaltung der Compliance mit der DSGVO ist.
Verhaltensregeln	Allgemeine oder branchenspezifische Verhaltensregeln und Zertifizierungen bieten Unternehmen nützliche Anleitung zu Ansätzen im Hinblick auf Datenschutzprobleme.

Rechte von Einzelpersonen

Recht auf Informa-tion und ausdrück-liche Zustimmung	Einzelpersonen müssen über die Aufbewahrungsdauer ihrer personenbezogenen Daten sowie über ihr Recht, ihre Zustimmung jederzeit widerrufen und/oder eine Beschwerde einlegen zu können, informiert werden.
Recht, vergessen zu werden	Einzelpersonen sind berechtigt, ihre personenbezogenen Daten an mehreren Stellen und bei mehreren Verantwortlichen löschen zu lassen.
Recht auf Daten-portabilität	Einzelpersonen dürfen eine Kopie ihrer Daten in einem digitalen und weit verbreiteten Format vom Verantwortlichen anfordern, sodass diese bei Bedarf an einen Dritten weitergeleitet werden können.
Zustimmung zur Profilerstellung	Einzelpersonen haben das Recht darauf, dass Entscheidungen über sie nicht ausschließlich basierend auf ihrem Profil getroffen werden.

Datenschutz als Konzept

Modernste Cybersicherheit	Erstklassige Methoden, Prozesse und Technologien zur Sicherstellung von State-of-the-Art Cybersicherheit.

Expertenmeinung

Internationaler Gültigkeitsbereich der DSGVO und Nachweis der Compliance

Lothar Determann, Rechtsanwalt und Experte auf dem Gebiet der Compliance mit Datenschutzgesetzen, gibt im folgenden Auszug aus der dritten Auflage seines Ratgebers *Datenschutz: International Compliance Field Guide*, der später dieses Jahr erscheint, einen allgemeineren Überblick über den Gültigkeitsbereich der DSGVO:

„Im Mai 2018 tritt die neue EU-Datenschutz-Grundverordnung (DSGVO) in allen Mitgliedsstaaten des Europäischen Wirtschaftsraums („EWR“) in Kraft. Dies wirkt sich unmittelbar auf Unternehmen aus. Viele Unternehmen außerhalb des EWR sind ebenfalls von der DSGVO betroffen, etwa, wenn sie personenbezogene Daten von Verbrauchern aus dem EWR erfassen.

In der DSGVO, der ersten größeren Neufassung der EU-Datenschutzgesetze seit 1995, sind harte Strafen vorgesehen. Außerdem bringt sie wichtige Änderungen für Unternehmen, darunter folgende:

- Unternehmen müssen Folgenabschätzungen für die Verarbeitung vertraulicher Daten durchführen sowie sämtliche Aktivitäten der Datenverarbeitung und Bemühungen zur Compliance in vordefinierten Datensatzformaten dokumentieren. Dies umfasst die Kategorien der Daten und betroffene Personen, die Zwecke der Verarbeitung, Empfänger, internationale Übermittlungen und angemessene Schutzmaßnahmen, Zeitgrenzen für die Löschung sowie technische und organisatorische Sicherheitsmaßnahmen (Art. 5, 30, 35). Unternehmen sind gezwungen, eine Dokumentation als Nachweis der Compliance vorzubereiten sowie Lücken zu erkennen und zu schließen.
- Unternehmen außerhalb des EWR müssen einen Vertreter innerhalb des EWR benennen, was sie in viel höherem Grad der lokalen Rechtsprechung und Verfügbarkeit aussetzt.
- Unternehmen müssen robuste Programme zur Datenhaltung und Delegierung umsetzen, um strengere Regeln für den Zugriff, die Korrektur und Löschung von Daten einzuhalten.
- Unternehmen müssen betroffenen Personen detailliertere Datenschutz-Mitteilungen bieten und dabei die Identität sowie Kontaktinformationen des Datenverantwortlichen (für ausländische Unternehmen zudem den Vertreter im EWR), die Kontaktinformationen des Datenschutzbeauftragten, die Zwecke und Rechtsgrundlage der Datenverarbeitung, das berechtigte Interesse des Verantwortlichen oder Dritten – falls dies die Grundlage zur Rechtfertigung der Verarbeitung darstellt –, die Empfänger oder Empfängerkategorien, für internationale Datenübermittlungen das Vorhandensein oder Fehlen einer angemessenen Entscheidung durch die Kommission und Informationen zu Schutzmaßnahmen sowie viele weitere Details bereitstellen.

Neben der DSGVO müssen Unternehmen weiterhin nationale Datenschutzgesetze einhalten. Im Gegensatz zur Datenschutzrichtlinie von 1995 gilt die DSGVO direkt für Unternehmen, ohne Umsetzung in nationales Recht. Allerdings können durch nationale Gesetze weitere oder strengere Regeln aufgestellt werden, die bis zur Widerrufung gültig bleiben. Mehr als 50 Abschnitte in der DSGVO ermöglichen es Staaten, detailliertere oder strengere Regeln zu verschiedenen Themen einzusetzen. Die DSGVO dient dazu, europäische Datenschutzgesetze zu vereinheitlichen, und hat das Potenzial dazu, wenn die Mitgliedsstaaten des EWR vorhandene nationale Gesetze zugunsten der neuen DSGVO zurückziehen. Allerdings behalten einige EWR-Mitgliedsstaaten vorhandene Gesetze bei und sorgen so für Unsicherheit bezüglich des Ausmaßes der Bevorrechtigung und Harmonisierung. Ein weiterer Unsicherheitsfaktor in Europa ist der Austritt Großbritanniens aus der EU, was zur Einführung abweichender Datenschutzgesetze in einer der wichtigsten Rechtsprechungen in Europa nach der Größe ihrer Bevölkerung und Wirtschaft führt.“

Lothar Determann,
Datenschutzexperte

Der Ausspruch „Daten - Das neue Öl“ ist immer passender in der Welt des elektronischen Business und Onlinehandels, doch es ist schwer, sich „reich zu handeln“, denn Daten in Unternehmen sind oft zu unverarbeitet, aufgeteilt, begrenzt zugänglich und schwierig aufzufinden. Bei zentralisierten Daten geht es um den passenden, konsolidierten Satz Daten, im richtigen Format, mithilfe von Statistiken auswertbar, um daraus Erkenntnisse für Geschäftsentscheidungen zu ziehen und sich im Endeffekt einen Wettbewerbsvorteil zu verschaffen. Innerhalb des Rahmenbaus der DSGVO sind EU-Bürger Eigentümer ihrer personenbezogenen Daten und „verleihen“ sie nur an Unternehmen. Sie machen sich Sorgen über die Nutzung ihrer Daten und sind bereit, mit Unternehmen zu interagieren, denen sie vertrauen und bei denen sie die größten Schutzmaßnahmen für ihre Daten wahrnehmen. Um sicherzustellen, dass die Datenverarbeitung sich nicht negativ auf die Rechte betroffener Personen auswirkt, und dass personenbezogene Daten jederzeit geheimgehalten werden, bezieht sich die DSGVO oft auf das Konzept der "modernen Sicherheit". Es basiert auf die stetige Weiterentwicklung bewährter Vorgehensweisen und Technologien, in denen mehrere Schutzebenen für Daten gelten, sodass eine große Bandbreite an Risiken abgedeckt werden, darunter folgende:

Für globale Unternehmen vereinheitlicht die DSGVO den aktuell fragmentierten rechtlichen Rahmen für Datenschutz in der EU, indem sie eine einheitliche Datenschutz-Grundverordnung bietet, die sowohl Datensicherheit als auch die Geschäftsergebnisse für Großunternehmen abdeckt. Wichtig ist: Die Verordnung verlangt in gleicher Weise auch von kleinen und mittelständischen Unternehmen (KMU) die Verwaltung ihrer Datenströme, Übermittlungen und Prozesse, um die Verordnung vollständig einzuhalten. Wie von ihren größeren Gegenstücken wird von KMU erwartet, die Risiken ihrer geschäftlichen Vorgehensweisen in Bezug auf den Datenschutz betroffener Personen auszuwerten, ihre Interessen an den Rechten betroffener Personen auszurichten und eine vollständige Dokumentation bereitzustellen, durch die garantiert wird, dass diese Erwägungen in den Prozess der Entscheidungsfindung integriert sind. Unternehmen mit weniger als 250 Mitarbeitern durch die DSGVO werden bestimmte Ausnahmen erlaubt, was an den geringeren Risiken liegt, die sie im Vergleich zu größeren Unternehmen darstellen. Daher sind Aufsichtsbehörden in jedem Land aufgefordert, die besonderen Bedürfnisse von KMU bei der Anwendung der DSGVO zu berücksichtigen. Beispielsweise sind Unternehmen mit weniger als 250 Mitarbeitern vom Führen einer Akte über die verarbeiteten Aktivitäten befreit, und EU-Mitgliedsstaaten können entscheiden, ob solche Unternehmen einen Datenschutzbeauftragten benennen müssen.

Stellt die DSGVO neue Risiken heraus?

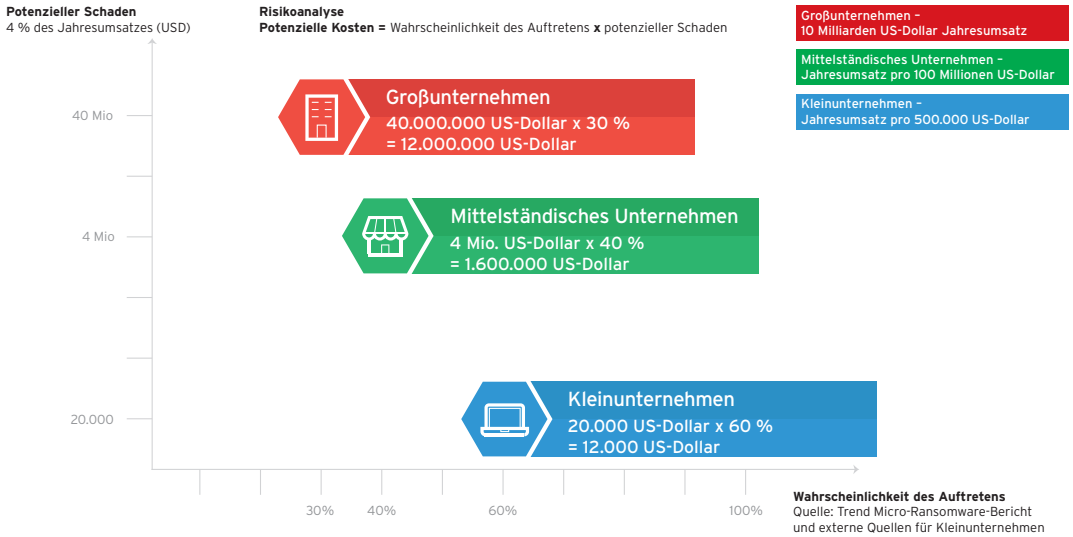
Bei Projekten zur Einhaltung der DSGVO müssen Technologietrends und auf dem Markt aufkommende Nutzungsmuster berücksichtigt werden. Im klassischen IT-Umfeld sind personenbezogene Daten innerhalb bekannter Grenzen verblieben. Doch da das Internet of Things (IoT), Mobilität und die Cloud allgegenwärtig werden, sind Daten auf mehrere Umgebungen verteilt, und Datenströme werden zu einem stets präsenten Teil der IT. Die Bewertung von Daten, die fälschungssicheren Schutz erfordern, kann daher eine Herausforderung darstellen, und sie zu schützen ist noch komplexer, denn es mangelt an Transparenz.

In der jährlichen Studie zu Datenschutzverletzungen 2016 meldete das Ponemon Institute immer höhere Kosten von Datenschutzverletzungen, die sich nunmehr auf 4 Millionen $ pro Vorfall summieren, ein Anstieg um 29 % seit 2013[2]. Zu den zugehörigen Kosten zählen mehrere Punkte, etwa die Untersuchung, Abhilfe, forensische Analysen, Benachrichtigungen an die betroffenen Parteien, Unterstützung usw. Die DSGVO führt eine weitere Kostenebene ein, denn in der Verordnung werden beträchtliche administrative Strafen festgelegt, die bei Nichteinhaltung fällig werden. Da in der Verordnung zwei Stufen Geldstrafen beschrieben werden, kann der Betrag der Strafen beträchtlich hoch sein und sich stark auf das Unternehmen auswirken.

Um einen Einblick in die Kosten einer Datenschutzverletzung im Kontext der DSGVO und der Größe eines Unternehmens zu geben, werden in der nachfolgenden Grafik die Wahrscheinlichkeit einer Verletzung sowie die Größe des Unternehmens zur Ermittlung der potenziellen Kosten berücksichtigt. Während die Höhe der Strafen laut

der DSGVO können sich potenziell beträchtlich auf die finanzielle Haftbarkeit eines Unternehmens auswirken und sind in vielen EU-Staaten wahrscheinlich deutlich höher als vorgeschrieben. Die Durchsetzung von Strafen durch nationale Aufsichtsbehörden wird mit einer Bewertung der Fähigkeit eines Unternehmens kombiniert, dessen Intention zur Einhaltung der DSGVO zu beweisen.

2 Ponemon Institute "2016 Cost of Data Breach Study: Global Analysis", Juni 2016



Wichtig ist: Die Folgen einer Nichteinhaltung können über Geldstrafen hinausgeben und sogar zu einer Anordnung führen, die Datenverarbeitung einzustellen, was für verarbeitungsintensive Vorgänge katastrophal wäre. Unternehmen sollten die Tatsache nicht übersehen, dass die DSGVO betroffenen Personen in bisher ungekanntem Ausmaß Rechte verleiht und so z. B. die Einreichung von Beschwerden ermöglicht, die weitere finanzielle und markenrechtliche Schäden fördern könnten. Schließlich sollten auch die Risiken für den Ruf bedacht werden, denn Kunden verlangen danach, mit Unternehmen zu tun zu haben, die ihre Daten rechtmäßig verarbeiten und Anfragen zur Löschung oder Übermittlung von Daten unterstützen.

WannaCry: ein früher Weckruf für die DSGVO

Im Mai 2017 überraschte die Ransomware WannaCry viele Unternehmen in aller Welt, und einige erlebten daraufhin einen kompletten Geschäftsausfall. Diese Malware verschlüsselte Unternehmensdaten – darunter auch personenbezogene Daten – auf angreifbaren Systemen und forderte ein Lösegeld. Dieses Ereignis kam in die Schlagzeilen der internationalen Medien und bezeugt, dass viele Unternehmen weiterhin für fortschrittliche Angriffe verwundbar waren.

Kann die bösartige Verschlüsselung von Daten in Zusammenhang mit Verletzungen des Schutzes personenbezogener Daten laut Definition in der DSGVO gesehen werden? Die Antwort lautet JA, denn in Art. 4.12 der Verordnung wird ein solcher Vorfall definiert als „eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet werden“. Dies führt zu einer weiteren Frage: würden betroffene Unternehmen strafrechtlich verfolgt und mit Geldstrafen belegt, falls eine Attacke ähnlich wie WannaCry erneut auftritt, nachdem die DSGVO in Kraft getreten ist? Die Wahrscheinlichkeit dafür ist hoch, denn bekannt ist, dass die Opfer die bekannte Windows-SMB-Sicherheitslücke, die von der Ransomware genutzt wurde, nicht geschlossen hatten. Natürlich verlangt die DSGVO nicht ausdrücklich von jedem Unternehmen, die eigenen Systeme zu aktualisieren, doch dies wird als Best Practice in der Branche angesehen, um Exploits zu verhindern. Falls das Patchen scheitert oder keine Technologie für virtuelles Patchen verfügbar ist, wird es recht schwierig, die Behörden davon zu überzeugen, dass beste Bemühungen zum Schutz personenbezogener Daten angewendet wurden.

Der Ablauf zur Einhaltung

Daten sind von Natur aus dynamisch und verlangen nach einem ähnlich dynamischen Ansatz zum Schutz. Mehrere Branchenumfragen wurden seit der Einsetzung der DSGVO im April 2016 durchgeführt, in denen der Grad der Bereitschaft und das Wissen in Unternehmen bewertet wurden. Im August 2017 bestätigte Gartner die Ansicht, dass über 50 Prozent der globalen Unternehmen, die von der DSGVO betroffen sind[3], selbst bis Ende 2018 nicht konform sein werden. Eine 2017 von Trend Micro durchgeführte internationale Umfrage bestärkte diesen Standpunkt und zeigte eine Lücke des allgemeinen Verständnisses, denn fast 67 Prozent der Unternehmen sind sich der Höhe möglicher Strafen und Sanktionen im Rahmen der DSGVO nicht bewusst. Zudem wussten 42 Prozent der Teilnehmer nicht recht, was personenbezogene Daten ausmacht (z. B. verstanden sie nicht, dass eine E-Mail-Marketingdatenbank personenbezogene Informationen enthält). Dies sind zwar deutliche Frühwarnsignale, doch die Chance, bis zur Durchsetzung der DSGVO im Mai 2018 Compliance zu erzielen, ist noch sehr real.

Expertenmeinung

Die Einhaltung der DSGVO bezieht viele Beteiligte mit bewährtem Fachwissen in den Bereichen Betrieb, Recht und Technik mit ein, doch der Leiter dieses Projekts ist jetzt der Datenschutzbeauftragte, eine neue Rolle, eingeführt durch die DSGVO. In dieser übergreifenden Funktion ist es nötig, dass der Datenschutzbeauftragte – ob angestellt oder mit einem Servicevertrag – eng mit allen Beteiligten zusammenarbeitet und volle Unterstützung der Geschäftsleitung hat, um die nötigen Ressourcen einzubinden und darauf zu achten, dass die Compliance mit der DSGVO eine hohe Priorität behält. Je nach ihrer Größe, Branche und weiteren Besonderheiten müssen Unternehmen ihr eigenes angepasstes Compliance-Programm einsetzen. Für die meisten Unternehmen geht es bei der Umsetzung der DSGVO um beträchtliche organisatorische Ressourcen, eine Veränderung der Datenprozesse sowie eine Investition in Sicherheitsverfahren und -technologien – eine einzelne Technologie, die Compliance in allen drei wichtigen Bereichen erzielen würde, die es zu berücksichtigen gilt, gibt es nicht:

RECHT UND COMPLIANCE

Die DSGVO führt neue Anforderungen für Funktionen zur rechtlichen Compliance ein. In vielen Unternehmen wird ein Datenschutzbeauftragter Pflicht, der eine Schlüsselrolle zur Sicherstellung der Compliance spielt. Geschätzt 28.000 neue Datenschutzbeauftragte werden allein in Europa benötigt. Bei Nichteinhaltung der DSGVO sehen sich Unternehmen den höchsten Strafen gegenüber, die es jemals gab – bis zu 4 % des Jahresumsatzes. Ein erneuter Fokus auf der Verantwortung der Unternehmen erfordert einen proaktiven, robusten Umgang mit Datenschutz: Unternehmen sollten überprüfen, wie sie ihre Datenschutzrichtlinien verfassen, damit sie leichter verständlich sind.

- Allgemeiner Berater/Recht
- Datenschutzbeauftragter
- Leitender Risikobeauftragter
- Leitender Compliance-Beauftragter

TECHNOLOGIE

Neue Anforderungen durch die DSGVO bedeuten Änderungen an der Art und Weise, wie Technologien entworfen und verwaltet werden. Dokumentierte Datenschutz-Folgenabschätzungen werden zur Bereitstellung neuer Systeme und Technologien erforderlich. Sicherheitsverletzungen müssen binnen 72 Stunden an die Behörden gemeldet werden, was die Umsetzung neuer oder verbesserter Verfahrensweisen zur Reaktion auf Vorfälle erfordert. Das Konzept des „Datenschutzes als Konzept“ wurde im Gesetz verankert, und man erwartet, dass die Datenschutz-Folgenabschätzung in den nächsten paar Jahren zum Standard wird. Zusätzlich wird von Unternehmen erwartet, dass sie Datenmaskierung, Pseudonymisierung und Verschlüsselung in Erwägung ziehen.

- Chief Information Officer
- Chief Information Security Officer
- Chief Technology Officer

DATEN

Einzelpersonen und Teams, deren Aufgabe das Informationsmanagement ist, stehen vor der Herausforderung, einen klareren Überblick über die Datenspeicherung, Übermittlungswege und Herkunft der Daten zu liefern. Wer einen klaren Blick dafür hat, welche Daten erfasst und wo sie gespeichert werden, kann neue Rechte betroffener Personen leichter erfüllen – das Recht, die eigenen Daten löschen und/oder an andere Unternehmen übertragen zu lassen.

- Chief Data Officer
- Chief Operating Officer
- Chief Marketing Officerr
- Data Stewards
- Digital Leads

Daher empfehlen führende Beratungsunternehmen wie Deloitte, die Compliance mit der DSGVO als Rahmenbau mit Aufgaben zu betrachten, anstelle nach einer Technologie zu suchen, die das Problem wie ein Allheilmittel löst. Mit dieser Empfehlung im Sinn sollten Unternehmen jetzt damit beginnen, tätig zu werden. Die nachfolgende Liste ist zwar nicht erschöpfend, bietet aber einen übersichtlichen Rahmen für Aktionen, die Unternehmen durchführen sollten, um Compliance zu erzielen:

Bewusstsein der Beteiligten

Stellen Sie sicher, dass alle Beteiligten sich voll der DSGVO und ihrer Auswirkungen auf das Unternehmen bewusst sind. Achten Sie darauf, dass die wichtigen Botschaften vom Vorstand und den Führungskräften verstanden werden – und holen Sie sich Zustimmung für Anpassungs- und Änderungsprogramme.

Datenbestände und Zuordnung

Erstellen Sie eine Bestandsliste der personenbezogenen Daten, die erfasst werden, mit wem sie geteilt werden und welche Kontrollen für ihre Nutzung gelten. Die Behörden erwarten, dass diese Daten stets parat stehen.

Bewertung der Bereitschaft

Führen Sie eine Bewertung der Bereitschaft durch, um zu erkennen, wie nah oder weit Ihr Unternehmen von relevanten neuen Anforderungen der DSGVO entfernt ist, und bewerten Sie den potenziellen Aufwand.

Zuständigkeit

Nutzen Sie die DSGVO, um Ihren Ansatz in Sachen Datenschutz als Ganzes zu bewerten – gibt es in Ihrem Unternehmen einen Datenschutzbeauftragten? Wer ist schlussendlich verantwortlich? Wie bringen Sie verschiedene Geschäftsbereiche zusammen, um die Risiken für den Datenschutz fortlaufend zu verwalten?

Recht und Compliance

Überprüfen Sie, wie Sie die Zustimmung von Nutzern einholen. Überarbeiten Sie Datenschutzerklärungen und legen Sie fest, wie die Compliance gezeigt wird.

Technologie

Stellen Sie Technologien und Verfahrensweisen bereit, die zum „Datenschutz als Konzept“ passen, und stellen Sie robuste Verfahrensweisen zum Umgang mit Schutzverletzungen auf, darunter Maskierung und Verschlüsselung.

Daten

Achten Sie darauf, dass in Ihrem Unternehmen die passenden Datenzuständigkeitsrichtlinien zum Einsatz kommen, sodass Sie effizient auf die neuen Rechte eingehen können, die betroffenen Personen eingeräumt werden, wie z. B. das Recht auf Löschen und Übertragen der Daten.

Unternehmen müssen die lange Liste der Anforderungen der DSGVO in eine Reihe anzugehender Arbeitspakete aufspalten und für jedes dieser Arbeitspakete einen Zielstand festlegen, für den sichtbare Ergebnisse bis 25. Mai 2018 erzielt werden. Dies sollte von einem Blick darauf ergänzt werden, welcher Zielstand langfristig angesteuert werden sollte, wenn neue Datenschutzbestimmungen aufkommen. Mehrere Beteiligte an einen Tisch zu bringen und die Zuständigkeiten für die Umsetzung klar zu verteilen, festzulegen, wie risikofreudig das Unternehmen ist, und sich über einen Gültigkeitsbereich einig zu werden ist nicht immer einfach, wenn man die unterschiedlichen Hintergründe und Blickwinkel bedenkt, die jeder mitbringt.

Nur allzu oft entsteht eine Leere zwischen den Beteiligten, da die Rechtsabteilung vom Unternehmen erwartet, die Interpretation der Bestimmungen anzuerkennen und Änderungen herbeizuführen, während Geschäftsinhaber viel mehr Details darüber erwarten, was genau im Einzelnen getan werden muss. Die Ausrichtung von Mitarbeitern der Rechtsabteilung sowie aus dem Bereich „Risiko und Compliance“ mit Prozess- und Systemeigentümern ist hingegen wichtig, damit beide Seiten eine klar vereinbarte und nutzbare Reihe an Anforderungen und Ergebnissen haben.

Peter Gooch
Partner, Deloitte Cyber Risk Services

Datenschutz als Konzept

Datenschutz als Konzept – auch Datensicherheit als Konzept genannt – muss eines der Hauptleitprinzipien des Aktionsplans sein. Das führt dazu, dass Datenschutz von Anfang an zu einem integralen Bestandteil wird. Daher müssen Datenschutzverfahren und -technologien während der Konzeptphase von Informationstechnologien und -systemen eine hohe Priorität haben.

Laut Art. 25 der DSGVO sollten die technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten sich nach dem jeweiligen Risiko richten: je höher das Risiko, desto rigoroser die Maßnahmen, die der Verantwortliche oder Auftragsverarbeiter ergreifen muss. In der DSGVO wird die Risikogefahr mithilfe bestimmter Datenschutzparameter bewertet, die berücksichtigt werden müssen, insbesondere Natur, Reichweite, Kontext und Zwecke einer Datenverarbeitung. Außerdem wird das Risiko in der Verordnung klar den Maßnahmen gegenübergestellt, die zur Wahrung der Rechte und Freiheiten betroffener Personen getroffen wurden. Bei diesem Ansatz werden die Folgen einer potenziellen Verletzung des Schutzes personenbezogener Daten auf betroffene Personen als Schlüsselfacette der Risikobewertung betrachtet. Datenschutz als Konzept stellt zwar eine der größten Herausforderungen dar, denen Unternehmen begegnen, in denen Teams mit unterschiedlichen Hintergründen nicht an eine fortlaufende Zusammenarbeit gewöhnt sind. Er muss aber definitiv eine Priorität für die Cybersicherheits- und Marketingteams sein, wenn diese neue Geschäftsanwendungen entwerfen und unterstützen.

> „Wenn Notfall-Experten mühseligen Herausforderungen begegnen, sind sie nur allzu oft auf der Suche nach einer einzelnen Technologie, die das Problem lösen kann. Im Falle der Datensicherheit gibt es aber keine solche Technologie. Stattdessen benötigen Sie einen Rahmenbau, in dem dargelegt wird, wie Sie Daten entdecken, klassifizieren, analysieren und schließlich verteidigen und dazu eine Mixtur aus Sicherheitsprozessen, technischen Kontrollen und der Bereitschaft nutzen, eine Kultur zu schaffen, in der Datenschutz respektiert und geschätzt wird.“

Quelle: Forrester, Protect Your Intellectual Property and Customer Data From Theft And Abuse, Stephanie Balaouras , 12. Juli 2017

Visualisieren, wo die Daten liegen

Zum Start des Projekts zur Einhaltung der DSGVO müssen Unternehmen einen tiefen Blick in die eigenen Ressourcen werfen und ermitteln, wo personenbezogene Daten gespeichert werden und mit welchen Verfahrensweisen sie verarbeitet und ausgetauscht werden. Dann geht es darum, zu definieren, welche Daten besonderen Schutz benötigen. Kurz gesagt, diese Aufgabe ist mühsam und manchmal entmutigend: Daten, einst innerhalb der Grenzen klassischer Netzwerke abgelegt, sind heute überall und werden auf mobile Endpunkte, intelligente Geräte, in die Public Cloud, an Standorte von Partnern/Auftragsverarbeitern und an viele andere Orte übertragen. Die gute Nachricht ist: Technologie kann dabei helfen, das Projekt „Compliance" insgesamt zu einem Erfolg zu machen. Data Loss Prevention (DLP) ist eine Sicherheitstechnik, die Anwendungen, Systeme, Geräte und weitere Inhalte, etwa E-Mail-Systeme, Microsoft SharePoint-Server, Dateiserver und sogar SaaS-Anwendungen wie Microsoft Office 365 prüft und personenbezogene Daten aufspürt. Dies erfolgt mithilfe von Vorlagen, die bestimmte Formate, Schlüsselwörter oder Ausdrücke enthalten, nach denen gesucht wird, um Kreditkartendaten, persönliche Anschriften oder Sozialversicherungsnummern nachzuverfolgen, um nur einige Beispiele zu nennen. Dank dieser Automatisierung können personenbezogene Daten schneller und mit nur wenigen falschen Treffern gefunden werden.

Ein konsistenter Datenplan sollte nicht ausschließlich auf ruhenden personenbezogenen Daten basieren. Übertragene Daten einschließlich der Daten, die zwischen Systemen innerhalb eines Unternehmens oder zu/von Dritten fließen, müssen ebenfalls eingeordnet werden, um umfassende Transparenz zu erzielen. In diesem Stadium kann das DSGVO-Compliance-Team festlegen, welche Aktionen zur Sicherstellung des Datenschutzes nötig sind. Hier stellt DLP wiederum seinen Wert als Hilfsmittel auf ständiger Mission heraus und überwacht stetig alle potenziellen Offenlegungen von Daten mit dem Ziel, jegliche Aktionen zu stoppen, die zu einer möglichen Offenlegung führen könnten. Ist DLP also ein Allheilmittel? Kurz gesagt nein. Wie im Forrester-Zitat angeführt, müssen Unternehmen Compliance im Kontext einer Reihe von Aktionen und Technologien betrachten. Allerdings ist DLP unter Betrachtung folgender Punkte nicht ausreichend:

- Erstens wird DLP oft als Störung der Mitarbeiter betrachtet und in einigen EU-Mitgliedsstaaten womöglich nicht einmal toleriert, denn DLP kann gegen den Datenschutz von Mitarbeitern verstoßen. Das Problem liegt hier in der genauen Definition dessen, was sich überwachen lässt und was nicht.
- Zweitens muss die DLP durch Best Practices unterstützt werden. Diese umfassen die Anforderung, personenbezogene Daten auf bestmögliche Weise zu zentralisieren, um die Reichweite der zu schützenden Daten einzugrenzen und effiziente Zugangskontrolle und Back-up-Strategien umzusetzen.
- Drittens muss die DLP mit weiteren Technologien kombiniert werden, um ein angemessenes Maß an Sicherheit zu liefern. Dazu zählen Verschlüsselung, Erkennung von Datenschutzverletzungen, Überwachung der Dateiintegrität, Anwendungsüberwachung und Funktionen zur Verwaltung von Angriffen/Schwachstellen, um nur einige zu nennen.

Zusammenfassend lässt sich sagen: *Zwar sehen viele Unternehmen DLP als wichtige Technologie zur Durchsetzung der Compliance mit der DSGVO, doch diese lässt sich nur durch mehrere Sicherheitsebenen erreichen*.

Cybersicherheit im Kontext der DSGVO

Netzwerk- und Informationssicherheit werden von der DSGVO abgedeckt. Präambel 49 der Verordnung konzentriert sich auf die Kapazität eines Netzwerks oder Informationssystems, versehentlichen Vorfällen sowie bösartigen Aktionen standzuhalten, die die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit personenbezogener Daten kompromittieren, ob nun gespeichert oder in Übermittlung. Unautorisierter Zugriff auf personenbezogene Daten sowie jegliche unautorisierte Offenlegung solcher Daten werden als schwerwiegendes Problem betrachtet, sodass Verantwortliche und Auftragsverarbeiter zugehörige Risiken bewerten, die Sicherheit auf einem angemessenen Niveau halten und die Verarbeitung personenbezogener Daten auf einen begrenzten Bereich beschränken müssen.

Datenschutz als Konzept und als Standard erhält mit der DSGVO eine hohe Priorität - von Unternehmen wird erwartet, angemessene technische und organisatorische Maßnahmen zu ergreifen. In jegliche Systeme, die mit der Verarbeitung personenbezogener Daten in Zusammenhang stehen, muss Sicherheit direkt von der Designphase an integriert sein. Beispielsweise werden in Art. 32 Pseudonymisierung und Verschlüsselung als bewährte Methoden zum Schutz personenbezogener Daten herausgestellt, denn die Freigabe nicht auswertbarer, geskripteter Materialien wirkt sich nicht negativ auf betroffene Personen aus. Datenschutz-Folgenabschätzungen sind erforderlich, wenn eine Art der Verarbeitung, insbesondere mittels neuer Technologien, zu einem hohen Risiko für die Rechte und Freiheiten betroffener Personen führen kann. Diese Abschätzung muss die Maßnahmen enthalten, die zur Bewältigung von Risiken, zum Schutz personenbezogener Daten und zum Nachweis der Compliance ergriffen wurden (Art. 35).

In der DSGVO wird anerkannt, dass Technologien für Datensicherheit eventuell zum Schutz von Daten geeignet sind, woraus sich schlussfolgern lässt, dass bösartige Zugriffe auf Netzwerke und Daten sowie Malware und Cyberangriffe verhindert werden müssen. Praktisch gesagt bedeutet dies die Bereitstellung von Technologien für Cybersicherheit.

State-of-the-Art / „Stand der Technik“ ist ein Muss

Ein Konzept zieht sich wie ein roter Faden durch die gesamte Verordnung, denn es wird häufig erwähnt: der sog. „Stand der Technik“ beziehungsweise “State-of-the-Art” (Art. 25 und 32). Doch was ist State-of-the-Art? Das Cambridge Dictionary definiert ihn als „sehr modern und die neuesten Ideen und Methoden nutzend“, während die englische Wikipedia ihn als „höchstes Niveau der allgemeinen Entwicklung, z.B. eines Geräts, einer Technik oder einer Wissenschaft, das zu einer bestimmten Zeit erreicht wird“, beschreibt. Diese Definitionen unterscheiden sich zwar in den Details, doch beide fügen den Kontext der Zeit hinzu. Hier liegt die Idee zugrunde, dass der Stand der Technik sich im Laufe der Zeit ändert. Was heute als Stand der Technik angesehen wird, wird sich in Zukunft wahrscheinlich ändern. Wendet man den Begriff auf Cybersicherheit an, bedeutet das: Innovation ist der Vorkämpfer kontinuierlicher Entwicklung effizienter Sicherheitsmethoden und -technologien. Im Falle von Methoden werden Unternehmen dazu ermuntert, vorhandene Empfehlungen von Behörden zu nutzen: der CNIL[4] in Frankreich, der ICO[5] in Großbritannien oder der ENISA[6] auf europäischer Ebene, um nur einige zu nennen. Parallel haben führende Branchenanalysten und große Beratungsfirmen eine Reihe von Best Practices festgelegt, die Unternehmen dabei unterstützen, ein geeignetes Maß an Cybersicherheit als Teil des Compliance-Prozesses insgesamt zu erreichen.

Beste Tools und beste Suites: So tragen sie zur Moderne bei

In den vergangenen Jahrzehnten hat sich die Auswahl geeigneter Sicherheitstechnologien zu zwei unterschiedlichen Ansätzen hin entwickelt: Beste Suite und beste Tools – oder, einfach gesagt, entweder die Nutzung einer integrierten Anwendungssuite eines einzelnen Anbieters oder die Verwendung von Paketen unterschiedlicher Anbieter, die in ihrer jeweiligen Kategorie als der Beste gelten. Beide Ansätze haben ihre Vor- und Nachteile, was die Verwaltung der Komplexität, Integrationskosten und, was am wichtigsten ist, der Effizienz anbelangt. Doch die Frage lautet: Lässt sich moderne Sicherheit durch nur einen dieser Ansätze erzielen?

Diese aufgeheizte Debatte, eine der ältesten in der Unternehmens-IT, erscheint hinter den Kulissen irgendwie ironisch: Fast alle Unternehmen nutzen in der Praxis einen hybriden Ansatz, also eine Mischung aus Suite-basierten und einzelnen Lösungen, ausgewählt mit dem Ziel, moderne Cybersicherheit zu liefern. Bei Trend Micro hat diese Diskussion unsere Ansichten darüber geformt, was zum Erreichen der Moderne nötig ist, und uns geholfen, vier wichtige Antriebe zu erkennen: Features, Zusammenarbeit, Vollständigkeit und Anpassung des Umfelds.

2000-2002 wurden Sicherheitsfeatures wie Reputationsdienste, Antimalware, Verschlüsselung und Firewalls als Premiumfunktionen angesehen; im Laufe der Zeit und wegen immer ausgefeilterer Bedrohungen wurden jedoch zusätzliche Techniken, wie z. B. Verhaltensanalyse, maschinelles Lernen und hostbasierte IPS (tiefgehende Paketinspektion) entwickelt und bereitgestellt, was den Stand der Technik neu definierte. Wichtig ist: Kein Feature sollte für sich betrachtet werden, sondern als Teil eines zusammenwirkenden Prozesses, bei dem Sicherheits- und Intelligence-Daten von allen gemeinsam genutzt werden. In Sachen Vollständigkeit geht es darum, Sicherheit in drei Bereichen umzusetzen, die für die Sicherheit in Unternehmen wirklich von Belang sind: im Netzwerk, bei Benutzern und im Rechenzentrum sowie der Cloud. Threat Intelligence muss zwischen diesen Segmenten geteilt werden, um einen Angriff umfassend verstehen zu können. Zu guter Letzt liegt die Fähigkeit, die Ansätze der besten Tools und besten Pakete zu kombinieren und aufeinander abzustimmen. Dies wird erreicht, indem Unternehmen sich einem Umfeld von Partnern öffnen, in das Produkte von Drittanbietern – ob neu oder bereits vorhanden – sich leicht in dieses fortschrittliche Sicherheitsnetz der Zusammenarbeit integrieren lassen, das für Unternehmen nötig ist. Dank ihrer umfassenden Ausrichtung auf das Konzept des „Stand der Technik“ liefert die Trend Micro XGen™-Sicherheitsstrategie eine generationsübergreifende Mischung von Techniken zur Abwehr von Bedrohungen, jeweils einzeln zur rechten Zeit angewendet und gestützt von globalen Threat Intelligence-Daten.

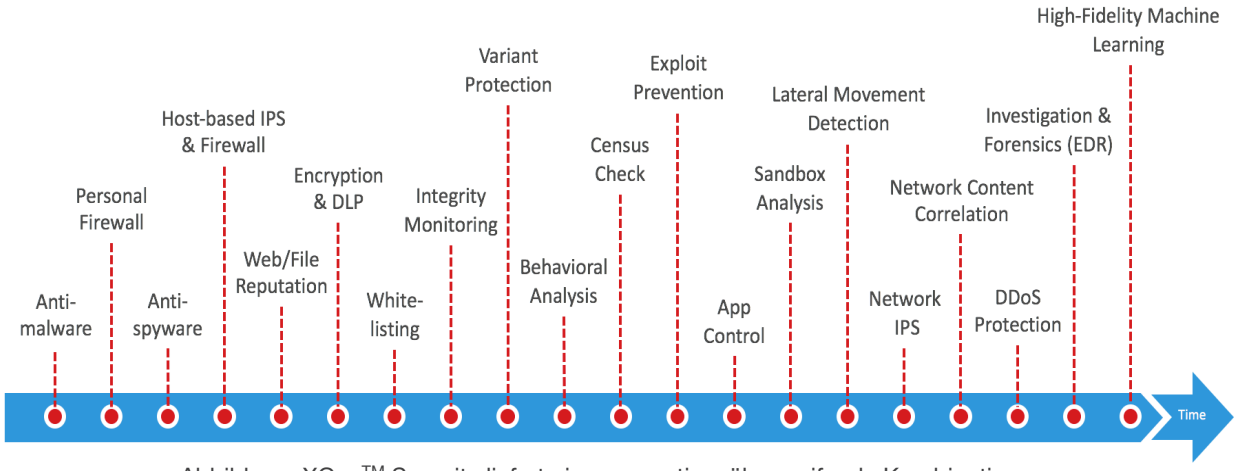


Abbildung: XGen™ Security liefert eine generationsübergreifende Kombination von Technologien zur Abwehr von Bedrohungen

Expertenmeinung

Pflicht zur Mitteilung von Verletzungen des Schutzes personenbezogener Daten sowie Bedarf für einen Reaktionsplan

Die DSGVO führt erstmalig eine EU-weite Pflicht zur Mitteilung von Verletzungen des Schutzes personenbezogener Daten ein. Bis jetzt gab es auf EU-Ebene branchenspezifische Verpflichtungen zur Mitteilung, die für Anbieter öffentlich verfügbarer elektronischer Kommunikationsdienste laut der ePrivacy-Richtlinie und für Betreiber grundlegender Dienste laut der Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie) galten. Zudem waren auch Meldepflichten für Datenschutzverletzungen in EU-Mitgliedsstaaten wie Deutschland und Großbritannien.

In der DSGVO werden Verletzungen des Schutzes personenbezogener Daten weiträumiger definiert als in vorhandenen Gesetzen zur Meldepflicht von Schutzverletzungen in den Vereinigten Staaten. Die Verordnung verpflichtet Datenverantwortliche, Aufsichtsbehörden und betroffene Personen über Verletzungen des Schutzes personenbezogener Daten zu benachrichtigen, außer die Schutzverletzung führt wahrscheinlich nicht zu einem hohen Risiko für die Rechte oder Freiheiten der betroffenen Person. Datenauftragsverarbeiter haben keine Meldepflicht gegenüber den Aufsichtsbehörden oder betroffenen Personen, müssen aber Datenverantwortliche umgehend über eine Verletzung des Schutzes personenbezogener Daten informieren. Einer der kontroversen Aspekte der neuen Anforderung besteht darin, dass die Aufsichtsbehörde, falls möglich, binnen 72 Stunden nach Erkennen einer Schutzverletzung durch den Verantwortlichen benachrichtigt werden muss. Verantwortliche müssen Verletzungen des Schutzes personenbezogener Daten dokumentieren, damit Aufsichtsbehörden die Einhaltung der Meldepflicht überprüfen können. Nichteinhaltung der neuen Verpflichtung ist ein erster Verstoß gegen die DSGVO und kann eine administrative Strafe von bis zu 10 Millionen Euro oder, im Falle eines Unternehmens, bis zu 2 % des weltweiten Gesamtjahresumsatzes ausmachen, je nachdem, welcher Betrag höher ist.

Die Umsetzung eines Programms zur Verwaltung von Datenschutzverletzungen stellt daher eine gute Geschäftspraktik dar und ist ein Bollwerk gegen diese Sanktionen. Zusätzlich zu diesen Strafen gibt es weitere ernste Folgen, etwa Beschwerden betroffener Personen, Schadenersatzansprüche, die Einstellung der Datenverarbeitung und beträchtlichen Reputationsverlust. Ordnungsgemäße Richtlinien, Vorgehensweisen, Prüflisten, Vorlagen und Dokumentationen sind der Schlüssel dazu, die Meldepflichten für Datenschutzverletzungen laut der DSGVO – sowie ähnliche Pflichten in anderen Rechtsprechungen aus aller Welt – und kurze Meldefristen einzuhalten. Bekanntheitskampagnen und Schulungen für Mitarbeiter sind wichtig. Das Programm sollte auch getestet und bei Bedarf regelmäßig überprüft und aktualisiert werden.

Als Vorbereitung auf potenzielle Schutzverletzungen müssen Verantwortliche und Auftragsverarbeiter vorhandene technische und organisatorische Sicherheitsmaßnahmen bewerten und ergänzen. Maßnahmen wie Verschlüsselung können ggf. sogar verhindern, dass der Verantwortliche betroffene Personen über eine Verletzung des Schutzes personenbezogener Daten benachrichtigen muss. Zudem sollten Unternehmen die Auswahl der genutzten Dienstanbieter überprüfen und dabei darauf achten, dass angemessene Sorgfaltsverfahren Datenschutz und -sicherheit abdecken. Unternehmen sollten dazu geeignete Vertragsbestimmungen aushandeln und deren Einhaltung überwachen. Die Verantwortungsbereiche sollten im Voraus an ein abteilungsübergreifendes Team zugewiesen werden, das sich aus Mitarbeitern der Bereiche Recht, Compliance, IT-Sicherheit, Personalwesen und Kommunikation zusammensetzt. Unternehmen wird auch empfohlen, sich im Voraus PR-Firmen, Kreditwürdigkeitsdienste, Forensikfirmen, Dienstleister für Öffentlichkeitsarbeit und externe Berater (Rechtsprivileg) anzusehen. Schließlich sollten Versicherungspolicen überprüft werden, um sicherzugehen, dass sie die Kosten einer Datenschutzverletzung ausreichend abdecken.

Monika Kuschewsky, Partner in der Data Privacy & Cybersecurity Practice, Squire Patton Boggs

Bereit für die DSGVO dank intelligenter, optimierter und vernetzter Abwehr

Die Abwehr moderner, fortschrittlicher Malware und zielgerichteter Angriffe erfordert, dass Sie Ihre aktuelle IT-Lösungsstrategie überdenken und sich für einen Ansatz entscheiden, der ein breites Spektrum an Umfeldern integriert und aussagekräftige Sicherheitsanalysen, gemeinsame Nutzung von Bedrohungsdaten, Zusammenarbeit zwischen Lösungen, bewährte Funktionen zur Reaktion auf Vorfälle sowie zentralisierte Transparenz über das gesamte Sicherheitsarsenal bietet.

Ihre Abwehr muss

INTELLIGENT SEIN

Eine intelligente Abwehr nutzt eine generationsübergreifende Kombination aus Techniken zur Verteidigung gegen Bedrohungen, die mehrschichtig sind und dadurch personenbezogene Daten vor bekannten und unbekannten Bedrohungen schützen können, ob die Daten ruhen, übertragen werden oder sich in einem beliebigen Schritt der Verarbeitung befinden. Zwar werden im Lauf der Zeit neue Sicherheitstechniken eingeführt, die neue Bedrohungen abwehren, doch die aktuellen Techniken sind weiterhin relevant und nötig zum Schutz der Daten. Dank generationsübergreifenden Kombination aus Techniken kann für jede Bedrohung die jeweils passendste und effizienteste Technik eingesetzt werden – denn eine Allheilmittel für die Sicherheit gibt es nicht.

Ihre Abwehr muss

OPTIMIERT SEIN

Optimierung ist während der Bereitstellung Ihres Abwehrmechanismus wichtig: Ihre Sicherheit muss eng mit der Datenverarbeitungsschicht vernetzt sein, und zwar über Techniken, die sowohl klassische als auch neue Unternehmensumgebungen wie die Cloud und Container effizient schützen. Diese Optimierung bietet Transparenz für Benutzer, Server und Netzwerke und ermöglicht es Unternehmen, die Auswirkungen von Bedrohungen zu analysieren und zu bewerten, den Stand in Sachen technische Sicherheitsinfrastruktur zu beurteilen und sich schnell einen Überblick über Vorfälle zu verschaffen, die im Unternehmen aufgetreten sein können.

Ihre Abwehr muss

VERNETZT SEIN

Eine vernetzte Abwehr hilft dabei, Datenschutzverletzungen zu verhindern und zu mindern, indem Daten über Bedrohungen sowie automatische Sicherheitsupdates über alle Sicherheitsebenen in Echtzeit geteilt werden. Dieser proaktive Ansatz stoppt Malware – wie z. B. Ransomware –, bevor personenbezogene Daten betroffen sein können. Infizierte Systeme, auf denen personenbezogene Daten gespeichert sind, werden isoliert, und bösartiger Traffic, der personenbezogene Daten abrufen, verändern oder löschen könnte, wird blockiert.

Eine intelligente, optimierte und vernetzte Abwehrstrategie schützt das Unternehmen über die gesamte Lebensdauer von Bedrohungen hinweg. Dies führt zu weniger Offenlegungen, erheblich kürzerer Lebenserwartung für Bedrohungen, die eindringen können, und viel weniger Aufwand und Kosten für die Reaktion auf Vorfälle. Dies ist eine Strategie, die klar beweist, dass ein Unternehmen in Sicherheit nach Stand der Technik als Teil der Einhaltung der DSGVO investiert hat.

So kann Trend Micro helfen

Durch Bereitstellung geeigneter Technologien können Unternehmen eine mehrschichtige Strategie für Cybersicherheit nach Stand der Technik umsetzen, die bei der Sicherstellung des Datenschutzes und der Compliance mit der DSGVO hilft. Projekte zur DSGVO-Compliance sind eine ideale Gelegenheit, zu überprüfen, wo ein Unternehmen mit Blick auf die Cybersicherheit insgesamt steht, und Verbesserungen umzusetzen, denn mehrere Anwendungsfälle müssen abgedeckt werden, um die Verordnung einzuhalten. Jeder Fall erfordert einen genauen Blick zur Bewertung der zugehörigen Risiken sowie eine Erwägung, welches der beste Ansatz dafür ist, personenbezogene Daten geheimzuhalten. Die folgenden Anwendungsfälle sind spezifische Beispiele, die zeigen, dass das breite Spektrum der Sicherheitslösungen von Trend Micro Ihnen Unterstützung auf Ihrem Weg zur Compliance bietet.

Schutz personen-bezogener Daten

Benutzer sind ein Hauptrisiko für den Verlust personenbezogener Daten. Daher sollten mehrere Szenarien in Betracht gezogen werden, einschließlich des versehentlichen Verlusts oder Diebstahls eines unverschlüsselten Laptops, mobilen Geräts oder Back-ups auf einem Flashspeicher. Daten können auch versehentlich offengelegt werden, wenn Benutzer personenbezogene Daten per E-Mail an einen Empfänger außerhalb des Unternehmens senden (insbesondere, wenn die E-Mail an den falschen Empfänger gesendet wird) oder wenn sie nicht zum Unternehmen gehörende Systeme nutzen, etwa persönliche Webmaildienste oder öffentliche Freigabewebsites. Daten können auch offengelegt werden, wenn ein Benutzer absichtlich einen Diebstahl begeht, wozu u. a. das Ausdrucken vertraulicher Dokumente oder das Kopieren zu schützender Informationen von Netzwerkservern oder einer Datenbank auf ein USB-Flashlaufwerk gehören.

Trend Micro-Lösungen für den Schutz personenbezogener Daten:

- Integrated Data Loss Protection (DLP) hilft bei der Erkennung und dem Schutz von personenbezogenen Daten
- Endpoint Encryption schützt personenbezogene Daten vor Diebstahl

Schutz von Mitarbeitern

Mitarbeiter können sich Identitätsdiebstahl durch Phishing und Social-Engineering-Angriffe ausgesetzt sehen, indem sie etwa Opfer einer E-Mail werden, die eine bösartige URL oder Anlage enthält. Sie sind auch angreifbar über Web-Exploits, Schwachstellen in Geräten und Betriebssystemen, Schwachstellen von Anwendungen sowie mit infizierten Flashlaufwerken. Und wenn sie eine bösartige Webseite besuchen, riskieren sie einen Drive-by-Download oder Exploit über den Browser bzw. ein Plug-in.

Trend Micro-Lösungen für den Schutz von Mitarbeitern:

- Email Security blockiert schädliche E-Mails
- Endpoint Security schützt Geräte der Nutzer vor bekannten und unbekannten Bedrohungen (Ransomware)
- Web Security schirmt Webbrowser-Aktivitäten ab
- Network Security blockiert Netz-Exploits und erkennt potenzielle Datenlecks

Schutz der Infrastruktur im Unternehmen

Die IT-Infrastruktur Ihres Unternehmens ist Zentrum zahlreicher Geräte, Server, Anwendungen, freigegebener Dateiserver, Datenbanken und vielem mehr – und alle sind potenzielle Ziele für Schutzverletzungen. Server und Anwendungen, die über das Internet erreichbar sind, lassen sich über Exploits und Schwachstellen in der Konfiguration infizieren und werden so zum Ausgangspunkt für die interne Weiterverbreitung. Der Schutz personenbezogener Daten in der gesamten IT-Infrastruktur erfordert den gestaffelten Einsatz mehrerer Sicherheitstechniken, darunter das Verhindern von unautorisiertem Zugriff auf Server und Anwendungen, in denen personenbezogene Daten verarbeitet oder gespeichert werden. Unternehmen sollten zudem auch Best Practices für die Sicherheit umsetzen, etwa die Verstärkung des Betriebssystems, das Ändern von Standard-Anmeldeinformationen sowie die Einrichtung von gesichertem Zugriff auf alle IT-Ressourcen.

Trend Micro-Lösungen für den Schutz der Infrastruktur im Unternehmen:

- Hybrid Cloud Security schützt Server und Anwendungen über das Rechenzentrum und die Cloud hinweg
- Network Security (via IPS) schirmt lokale Infrastruktur vor bekannten und nicht offengelegten Schwachstellen ab

Cloud-Datenschutz

In der Cloud und lokal sind die Risiken für die IT ähnlich (Exploits, schwache Sicherheitspraktiken usw.), doch die Verantwortung für die Sicherheit in der Cloud liegt gemeinsam beim IaaS-Anbieter und beim Unternehmen. Zwar bieten IaaS-Lösungen eine sichere Infrastruktur zur Ausführung von Workloads, doch für die Sicherheit gehosteter Anwendungen und in der Cloud verarbeiteter oder gespeicherter personenbezogener Daten ist der Kunde zuständig. Unternehmen sollten die integrierten Cloud- und SaaS-Konfigurationsoptionen in Kombination mit weiteren Sicherheitskontrollen nutzen, um so ihre Workloads und Daten in der Cloud zu schützen.

Trend Micro-Lösungen für den Schutz von Daten in der Cloud:

- Hybrid Cloud Security automatisiert den Schutz von Workloads über Multi-Cloud-Bereitstellungen
- Cloud App Security schützt SaaS-Umgebungen wie Office 365 vor Ransomware und Phishing

Schutzverletzungen erkennen und darauf reagieren

In der DSGVO wird gefordert, dass Datenschutzverletzungen nach ihrer Entdeckung an eine geeignete Aufsichtsbehörde gemeldet werden. Da heutige fortschrittliche Malware mehrere Verschleierungstechniken nutzt, nachdem sie sich Zugang zu einem Unternehmen verschafft hat, kann sie wochen- oder gar monatelang in einer IT-Infrastruktur schlummern, bis sie entdeckt wird. Um diese Lücke bis zur Entdeckung einer Schutzverletzung zu schließen, sollten Unternehmen ihre Umgebung engmaschig überwachen, wobei Hilfsmittel nach Stand der Technik zur Erkennung von Hinweisen auf Kompromittierung identifiziert und scheinbar nicht zusammenhängende, ziellose Aktionen als Ganzes betrachtet werden, um potenzielle Schutzverletzungen aufzudecken.

Trend Micro-Lösungen zur Erkennung von und Reaktion auf Sicherheitsverletzungen:

- Breach Detection System identifiziert verdächtige Aktivitäten, die zum Verlust von Daten führen können
- Connected Trend Micro-Lösungen in Benutzer-, Rechenzentrums- und Cloud-Umgebungen ermöglichen eine schnelle Reaktion auf und Behebung von Datenlecks

Das Puzzle zusammensetzen: Jetzt geht es los

> Am 25. Mai 2018 werden weniger als 50 % aller betroffenen Unternehmen vollständig mit der DSGVO konform sein.

Gartner, „GDPR Clarity: 19 Frequently Asked Questions Answered“, 29. August 2017

Im Mai 2018 tritt die DSGVO, ein Gesetz mit globalen Folgen, in Kraft. Das Gesetz soll die Rechte der Daten von Einzelpersonen schützen, ungeachtet dessen, wo das Ursprungsunternehmen seinen Sitz hat. Auf vielerlei Weise wird die Einsetzung der DSGVO Unternehmen helfen, länderübergreifend nur eine einzige Verordnung einhalten zu müssen, anstatt zu versuchen, unterschiedliche, widersprüchliche Gesetze einzuhalten, die heute existieren. Tatsächlich sagte die Europäische Kommission, die Verordnung werde Unternehmen jedes Jahr 2,3 Milliarden Euro sparen, da die Compliance bei der länderübergreifenden Ausübung von Geschäftstätigkeiten vereinfacht wird.

Der Weg zur Einhaltung birgt viele finanzielle, kulturelle und organisatorische Herausforderungen, von denen die größte darin besteht, sicherzustellen, dass die Compliance sich mit den Geschäftszielen vereinbaren lässt. Die Chance liegt in der Nutzung der vorgeschriebenen Änderungen zur Steigerung des Gesamtwerts des Unternehmens und der Marke, indem Daten bestmöglich und rechtmäßig genutzt werden. Um dies zu erreichen, muss sich der Ansatz zur Einhaltung allerdings über die zeitweilige Compliance hinaus mit dem Unternehmen weiterentwickeln. Die Verpflichtung zur Anwendung moderner Sicherheit laut DSGVO stellt eine Chance dar, die Compliance heute an Änderungen auszurichten, die in der sich stetig ändernden Welt der Bedrohungen ohnehin unvermeidbar sind.

Um Sie auf Ihrem Weg zur Einhaltung und darüber hinaus zu unterstützen, bietet Trend Micro Sicherheit nach Stand der Technik über unsere XGen™-Sicherheitsstrategie und ermöglicht es Unternehmen, Lösungen für Cybersicherheit zu nutzen, die Bedrohungen von heute und morgen begegnen und dabei zu den Anforderungen Ihres Unternehmens passen.

Die DSGVO ist zweifellos eine wichtige Änderung und Herausforderung, doch jede Änderung bringt auch Chancen mit sich. Dies wird eine Gelegenheit, die Personen umfassender zu verstehen, mit denen Sie Geschäfte tätigen und deren Daten von einem Unternehmen verwaltet werden, das bereit ist, neue, innovative Wege zur Interaktion mit ihnen zu finden. Zudem ist die DSGVO die ideale Chance, Cybersicherheit zu nutzen, um Ihr Unternehmen zu stärken und auszubauen.

Mitwirkende

Dieses Dokument ist das Ergebnis der Zusammenarbeit von Trend Micro-Experten weltweit. Wir haben auch Unterstützung von Dritten erhalten, wobei unser besonderer Dank Monika Kuschewsky, Peter Gooch und Lothar Determann für ihre Expertenbeiträge zu dieser Veröffentlichung gilt.

Monika Kuschewsky ist ein Partner bei Squire Patton Boggs. Als Rechtsanwältin und Certified Information Privacy Professional/Europe and Company Data Protection Officer ist sie auch Chefredakteurin von *Data Protection & Privacy – International Series*, einem Referenzleitfaden für mehrere Rechtsprechungen, veröffentlicht von Thomson Reuters für Unternehmen, Rechtsexperten und Datenschutzbeauftragte, der 46 wichtige Rechtsprechungen weltweit abdeckt.

Peter Gooch ist ein Partner der Deloitte Cyber Risk Services und spezialisiert auf Datenschutz, Datensicherheit und Cybersicherheit. Als Leiter der Datenschutz-Praxisabteilung von Deloitte UK verfügt Peter Deloitte über umfassende Erfahrung bei Datenschutzaufträgen und hat globale Datenschutz-Rahmenwerke bei einer Vielzahl multinationaler Unternehmen entwickelt und umgesetzt. Zudem hat er bereits viele Unternehmen bei ihrer Bereitschaft für die DSGVO unterstützt.

Lothar Determann praktiziert US-amerikanisches und deutsches Recht und berät globale Unternehmen seit mehr als 20 Jahren zur Compliance mit Datenschutzgesetzen. Er lehrt Computer- und Datenschutzrecht an der Freien Universität Berlin sowie an der University of California, Berkeley School of Law und Stanford Law School. Dieses Jahr erscheint die dritte Auflage seines renommierten Ratgebers *Datenschutz: International Compliance Field Guide*, in dem es erstmalig auch um die DSGVO geht.

Fußnoten und Referenzen

1. Tatsächlich gilt die DSGVO für den Europäischen Wirtschaftsraum (Staaten der Europäischen Union sowie Island, Liechtenstein und Norwegen).
2. Ponemon Institute „2016 Cost of Data Breach Study: Global Analysis“, Juni 2016
3. Gartner, „GDPR Clarity: 19 Frequently Asked Questions Answered“, 29. August 2017
4. https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes
5. https://ico.org.uk/for-organisations/data-protection-reform/
6. https://www.enisa.europa.eu/topics/data-protection
7. Europäische Kommission, 24. Mai 2017 – http://europa.eu/rapid/press-release_MEMO-17-1441_en.htm

TREND MICRO™

Trend Micro Incorporated ist ein Pionier auf dem Gebiet der Content Security und Bedrohungsbewältigung. Trend Micro wurde 1988 gegründet und bietet Einzelpersonen sowie Unternehmen aller Größen preisgekrönte Sicherheitssoftware, -hardware und -services bereit. Mit Firmensitz in Tokio und Niederlassungen in mehr als 30 Ländern werden Trend Micro-Lösungen vom Unternehmen sowie von Mehrwert-Vertriebspartnern und Serviceanbietern weltweit vertrieben. Weitere Informationen und Testversionen von Trend Micro-Produkten und -Services finden Sie auf unserer Website www.trendmicro.de.

TREND MICRO™

www.trendmicro.de/gdpr

©2017 by Trend Micro, Incorporated. Alle Rechte vorbehalten. Trend Micro und das Trend Micro t-Ball-Logo sind Warenzeichen oder registrierte Warenzeichen von Trend Micro, Incorporated. Alle anderen Produkt- und Firmennamen können Warenzeichen oder registrierte Warenzeichen der jeweiligen Eigentümer sein.